ADOA/ISD/AIS
Monthly Cyber Security Tips
NEWSLETTER

July 2007 Volume 2, Issue 7

Telecommuting Security Risks

From ADOA Information Security (AIS)

Background

Telecommuting is being used by some organizations for convenience or as part of a workforce, cost savings or environmental strategy or policy. The issue of telecommuting is increasingly coming to the fore due in part to the discussions of remote workforce capabilities. This paper is not advocating for or against telecommuting; however, if an organization does decide to implement telecommuting, there are steps that need to be taken to address security.

Security Issues/Risks

Telecommuting can consist of the employee connecting to his/her office network via their own home computer, or from an employer-issued machine. Because the employer has less control over the security of the employee's home computing environment than it does the office environment, there are specific risks that must be addressed. The user may not have installed the necessary components to keep software up-to-date and may not be checking the home computer regularly for viruses, trojans, adware or spyware. Individuals in the household other than the employee may access the computer and download or install software, unintentionally infecting it, including installing malware, such as keylogging utilities that can track sensitive information, such as user IDs and passwords. Other computers on the home network can become infected and potentially spread the infection to the telecommuting computer on the home network. In addition, users may have a wireless network at home which may not be adequately secured, thus making the devices on the wireless network open to intruders.

Another important security concern that should be addressed is the physical protection of the telecommuting computer or home computer and the data on the computer or on other storage media, such as CDs, DVDs, and USB flash drives. The computer and the devices may be stolen if a break-in occurs at the employee's house or vehicle.

Steps to Making Telecommuting Secure

Before allowing telecommuting, ensure that your organization has a telecommuting policy that addresses cyber security issues. The policy should define requirements for both employer and employee including a defined environment to work within.

1. The employer needs to decide whether to provide a computer to the employee. By providing the computer, the employer can control what is installed and what activities are allowed—or not allowed (such as instant messaging or peer-to-peer applications).
2. The telecommuting policy must state what security features must be installed and maintained on the computer. Best practice security features include the following:
    a. firewalls (software and/or hardware)
    b. anti-virus software
    c. anti-adware / anti-spyware software
    d. encryption software
3. The policy should state what software is needed for the employee to work remotely, as well as what types of software will not be allowed on the computer.
4. The policy should state to whom the user will report suspicious activity on the computer. Support

personnel should be ready to advise the employee on how to configure the computer and the employee's home networks for maximum security.

5. If the network connections are not properly secured, valuable data can be intercepted during the data transmission between the home and the office network. Virtual Private Networks (VPNs) are a best practice for securing communications to the organization's internal network. When connected to the organization's network, all transmissions should be encrypted, both coming from and going to the home. Every time a telecommuting device establishes a connection to the employer's network, it should be checked to ensure that all security software is active and up-to-date before being allowed access.
6. Organizations must assess the risk of allowing a telecommuter to directly access the organization's network vs. taking copies of the data home. If the data being taken home is personal, private or sensitive data, it should be encrypted.
7. If an organization has determined it will allow encrypted data to be removed from the network, organizations should limit the data being removed only to that which is absolutely necessary. In other words—don't download the entire file to bring home; only take that data which is absolutely necessary to complete the task.
8. As data is accessed from the organization's network by the telecommuting employee, the system should automatically log the time, date, user, computer or workstation, files, and the records they are accessing.
9. A two-factor method of authentication should be considered by the organization if the telecommuter accesses the organization's network from home.
10. The operating system and all applications should be up-to-date or at the most secure version available. File sharing should be turned off so no other computer can access data located on the telecommuting device.
11. Employees should be trained on security procedures.

Telecommuting Security Tips

1. Follow your organization's telecommuting policy.
2. Keep your anti-virus and anti-spyware/anti-adware software up-to-date and running real-time protection.
    a. Once a week, run a full scan on your computer – both anti-virus and anti-spyware.
3. Install a firewall and keep it up-to-date and configured securely.
    a. Talk with your organization's support personnel on how to configure it properly.
4. Report any suspicious activity on your computer such as:
    a. unexplained slow-down in performance
    b. ads popping up in windows
    c. hard-drive activity when you aren't running any applications
5. If your telecommuting computer was assigned to you by your organization, don't allow anyone else to access it.
6. If you have a wireless network at home, enable all security settings and change the default passwords.

Summary

Telecommuting is increasingly being discussed in today's work environment as organizations analyze remote workforce options. By taking precautions and enforcing a secure telecommuting environment, security risks can be minimized.

For more information:

http://csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf
http://www.itl.nist.gov/lab/bulletns/archives/telecomm.htm
http://www.fedtechmagazine.com/pf.asp?item_id=190
http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1147286,00.html?bucket=ETA

For previous issues of the Monthly Cyber Security Tips Newsletter go to www.msisac.org/awareness/news/

Brought to you by:

MS-ISAC

http://www.msisac.org